

### **DETAILED ACTION**

1. This is in response to the amendment filed November 21, 2008. Claims 11, 22, 27, 33 and 43 have been cancelled. Claims 1-10, 12-21, 23-26, 28-32, 34-42 and 44-55 are allowed. Claims 1-10, 12-21, 23-26, 28-32, 34-42 and 44-60 are pending and have been considered below.

#### ***Claim Rejections - 35 USC § 101***

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-10, 12-16, 49, 50 and 56-60 are rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, applicant's method steps are not tied to a particular machine and do not perform a transformation. Thus, the claims are non-statutory.

The mere recitation of the machine in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101. *Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.*

Claims 17-19 52 and 53 are non-statutory. The claims do not appear to include a hardware component to perform the function and thus appear to be relying on producing a useful, concrete, tangible result to establish a practical application. Claim 17 recites the step of providing, identifying, opening, determining, and performing without providing a hardware component.

Claims 33-37, 39-42, 44-48, 54, and 55 are drawn to a computer readable medium, which the applicant has defined in the specification (paragraph [0024]) to encompass an electronic transmission signal. The Office considers an electronic signal to be a form of energy. Energy is not a series of steps or acts and this is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a compilation of matter. Thus, an electronic transmission signal does not fall within any of the four categories of invention.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 56-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berger (US 2004/0123117) in view of Sobel (US 7,469,419).

**Claim 56:** Berger discloses a method for computer security, comprising:

identifying a file(paragraph [0084]);

- i. determining whether an entry for the file exists in database of unfamiliar software(*If the application characteristic doesn't match either a known safe application characteristic or a known unsafe application characteristic, a determination is made in operation 208 that the potentially unsafe application is an unknown application*)(paragraph [0047]; Fig. 3, steps 314-320);
- ii. adding an entry for the file to a database of known good software if the quantitative information exceeds a predetermined value(*if application is safe or unsafe operation 320, flow moves to an update local configuration operation 322. In update local configuration operation 322, the local configuration, e.g., application characteristics, on server system 130 is updated to reflect that the potentially unsafe application is now a known safe application or a known unsafe application*) (paragraphs [0068], [0081]); and
- iii. allowing the opening of the file to continue if the database of known good software includes the entry for the file(paragraph[0084]).

Berge does not explicitly disclose determining quantitative information regarding the file, the quantitative information selected from the group consisting of a length

of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed. However, Sobel discloses a method for determining if a file hash been infected, which determining quantitative information regarding the file, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed(column 1, lines 55 to column 2 6, column 2 lines 30-37; Fig. 5).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Berger such as to use quantitative information. The motivation of doing so would have been to improve the performance of malicious computer code detection as taught by Sobel (column 1, lines 5-10).

**Claim 57:** Berger and Sobel disclose the method as in claim 56 above, and Burger further discloses a step of removing the entry for the file from the database of unfamiliar software if the quantitative information exceeds a predetermined value(paragraph [0084]: Fig 2).

**Claim 58:** Berger and Sobel disclose the method as in claim 56 above, and Burger further discloses a step of preventing the opening of the file to continue if: the database of known good software does not include the entry for the file(terminating)(paragraph [0049]); and the file attempts a suspicious activity(deleting a file)(paragraph [0045]).

**Claim 59:** Berger and Sobel disclose the method as in claim 58 above, and Burger further discloses wherein a suspicious activity comprises updating a registry(paragraph [0033]).

**Claim 60:** Berger and Sobel disclose the method as in claim 58 above, and Burger further discloses wherein a suspicious activity comprises opening a second file(paragraph [0033]).

### ***Conclusion***

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Shipp US 2005/0080816 discloses a method for heuristically determining that an unknown file is harmless.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Art Unit: 2436

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Monday, March 16, 2009

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436